REMARKS

Claims 1 and 3-15 were presented for examination. Claims 1 and 3-15 stand rejected in the Office Action dated March 4, 2011 (herein, "OA"). Claims 1, 3, 7, 11-13 and 15 are amended herein. Claims 6 and 8 are canceled herein.

Response to Claim Objections

Claims 1 and 3-15 are objected to because of the following informalities: It appears that "and" is missing between the recited components, e.g. tangible personal digital key and a device. Claim 1 is amended to overcome this objection.

Claim 6 objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Claim 6 is canceled to overcome this objection.

Response to Rejections Under 35 U.S.C. § 112, 1st Paragraph

Claims 1 and 3-15 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. This rejection is overcome in view of the amended claims.

Amended claim 1 now recites, in part:

> …a device coupled to the personal digital key via a wireless network, the device including a second wireless transceiver that receives ~~data~~ a first activation code comprising a user label and an account number from the personal digital key and a reader/decoder circuit that transmits ~~data~~ the first activation code received from the tangible personal digital key to a key provider, the device receiving ~~data~~ digital content marked with an unlock code associated with the first activation code from a content

provider responsive to the key provider authenticating the first activation code received from the personal digital key and the device receiving data from the key provider indicating whether the first activation code is authenticated.

Support for the claim amendment is found throughout the specification. For example, page 11, line 3 to page 12, line 15 of the specification discloses:

> digital content available for purchase. To transmit the activation code to the content provider via the web site, the user may manually enter the activation code onto a secure page of the web site. Alternatively, the transmission of the activation code may be automatically implemented with wireless technology. Specifically, the user's computer may be outfitted with a detector that detects the activation code in the user's physical key and then relays the activation code to the content provider via the web site. The content provider may be affiliated with the key provider or may be separate from the key provider but have an arrangement therewith.
>
> Fifth, the content provider requests the key provider to verify the activation code transmitted by the user (step 18). The content provider may send this request to the key provider's web site. Sixth, the key provider in turn accesses the user's account in the user account database and determines whether the activation code is in fact valid (step 20). The key provider may also determine whether the activation code is associated with the user that transmitted the activation code to the content provider. If the activation code is rejected as being invalid, the content provider is so informed and the content provider in turn will not honor any request by the user to purchase digital content. If, however, the activation code is accepted as being valid, the content provider is so informed and the purchase transaction proceeds. As used herein, the term "key provider" generically refers to the entity or entities that manufacture, distribute, and validate the physical keys. These functions may actually be performed by multiple entities at different locations or by a single entity at a single location.
>
> Seventh, after securing validation of the first activation code in the physical key, the content provider pulls the requested digital content from a digital content database/library, marks the digital content with a second activation code (or unlock code) associated with the first activation code in the physical key, and encrypts the marked digital content (step 22). The second

activation code in the digital content may simply be the same as the first activation code in the physical key, but at least partially encrypted for security. In one embodiment, the "key-secured" content file includes the following data fields: user label, account number, and digital content. The user label and the account number serve as the second activation code for the digital content. If the content is merely for sampling (described in connection with FIG. 6), the file may include such additional data fields as a receiver/decoder circuit identification number, hour stamp, and life hours. All data fields on the content file, except for the user label, are preferably encrypted.

Eighth, the content provider delivers the encrypted digital content to the user (step 24). The encrypted digital content may be delivered by downloading the encrypted digital content to the user's computer while the user is online at the content provider's web site, by attaching the digital content to an e-mail addressed to the user, or by shipping a disk containing the encrypted digital content to the user via a package courier. The user may pay for the digital

Additionally, page 9, lines 7-16 of the specification discloses:

within the vicinity of RDC. The RDC reads the user's PDK key and transmits data, along with the user's account number, acquired using conventional techniques, to the provider for verification. If more than one PDK key is read at RDC, either data from all PDK keys is transmitted to the provider or User Labels are displayed on a computer screen to enable the user to select the appropriate PDK key. The provider looks up the account record in its database using the transmitted account number and compares the transmitted PDK key data to information stored in the record. If a match is confirmed, the transaction/session is completed normally. If not confirmed, the transaction/session cannot be completed.

Accordingly, various portions of the specification, such as the portions reproduced above, disclose a content provider transmitting a first activation code received from a PDK to a key provider that verifies if the first activation code is valid and informs the content provider. If the first activation code is validated, the content provider marks digital content requested by the PDK with a second activation code that is associated with the first activation code. Therefore, the specification contains a written description of the invention "in such full, clear, concise and exact terms as to enable any

person skilled in the art to which it pertains, or with which is it most nearly connected, to make and use the same," so reconsideration and withdrawal of the rejection of claim 1 is respectfully requested.

As claims 3-5, 7 and 9-15 depend from claim 1, all arguments advanced above regarding independent claim 1 are also applicable to dependent claims 3-5, 7 and 9-15. Thus, reconsideration and withdrawal of the rejection of claims 3-5, 7 and 9-15 is respectfully requested.

Additionally, the OA alleges that "further comprising a second personal digital key wherein the second digital key also authenticates a user attempting to access the device," recited by claim 5 is not disclosed in the original written disclosure.

However, claim 5 is amended herein to recite "further comprising a second personal digital key wherein the second digital key includes a third activation code comprising a user label associated with a second user and an account number associated with the second user." Support for the amendment to claim 5 is found throughout the specification. For example, page 9, lines 9-16 of the specification discloses:

> conventional techniques, to the provider for verification. If more than one PDK key is read at RDC, either data from all PDK keys is transmitted to the provider or User Labels are displayed on a computer screen to enable the user to select the appropriate PDK key. The provider looks up the account record in its database using the transmitted account number and compares the transmitted PDK key data to information stored in the record. If a match is confirmed, the transaction/session is completed normally. If not confirmed, the transaction/session cannot be completed.

Accordingly, various portions of the specification, such as the portion reproduced above, describes that more than one PDK keys are read at RDC and data from all PDK keys is transmitted to the provider, used for authentication. Therefore, the specification

discloses the cited term of claim 5, so reconsideration and withdrawal of the rejection of claim 5 is respectfully requested.

Response to Rejections Under 35 U.S.C. § 112, 2nd Paragraph

Claims 1 and 3-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. This rejection is respectfully overcome in view of the amended claims.

Amended claim 1 now recites, in part:

> …a device coupled to the personal digital key via a wireless network, the device including a second wireless transceiver that receives ~~data~~ a first activation code comprising a user label and an account number from the personal digital key and a reader/decoder circuit that transmits ~~data~~ the first activation code received from the tangible personal digital key to a key provider, the device receiving digital content marked with an unlock code associated with the first activation code from a content provider responsive to the key provider authenticating the first activation code received from the personal digital key and the device receiving data from the key provider indicating whether the first activation code is authenticated.

Accordingly, amended claim 1 more clearly recites that the second wireless transceiver in the device receives a first activation code comprising a user label and an account number from the personal digital key. The reader/decoder circuit in the device transmits the first activation code to the key provider and the device receives information from the key provider authenticating the activation code. Responsive to authentication of the first activation code, the device receives digital content marked with a second

activation code associated with the first activation code from a content provider. Support for this amendment is found throughout the specification.

For example, page 11, line 3 to page 12, line 15 of the specification discloses:

> digital content available for purchase. To transmit the activation code to the content provider via the web site, the user may manually enter the activation code onto a secure page of the web site. Alternatively, the transmission of the activation code may be automatically implemented with wireless technology. Specifically, the user's computer may be outfitted with a detector that detects the activation code in the user's physical key and then relays the activation code to the content provider via the web site. The content provider may be affiliated with the key provider or may be separate from the key provider but have an arrangement therewith.
>
> Fifth, the content provider requests the key provider to verify the activation code transmitted by the user (step 18). The content provider may send this request to the key provider's web site. Sixth, the key provider in turn accesses the user's account in the user account database and determines whether the activation code is in fact valid (step 20). The key provider may also determine whether the activation code is associated with the user that transmitted the activation code to the content provider. If the activation code is rejected as being invalid, the content provider is so informed and the content provider in turn will not honor any request by the user to purchase digital content. If, however, the activation code is accepted as being valid, the content provider is so informed and the purchase transaction proceeds. As used herein, the term "key provider" generically refers to the entity or entities that manufacture, distribute, and validate the physical keys. These functions may actually be performed by multiple entities at different locations or by a single entity at a single location.
>
> Seventh, after securing validation of the first activation code in the physical key, the content provider pulls the requested digital content from a digital content database/library, marks the digital content with a second activation code (or unlock code) associated with the first activation code in the physical key, and encrypts the marked digital content (step 22). The second

activation code in the digital content may simply be the same as the first activation code in the physical key, but at least partially encrypted for security. In one embodiment, the "key-secured" content file includes the following data fields: user label, account number, and digital content. The user label and the account number serve as the second activation code for the digital content. If the content is merely for sampling (described in connection with FIG. 6), the file may include such additional data fields as a receiver/decoder circuit identification number, hour stamp, and life hours. All data fields on the content file, except for the user label, are preferably encrypted.

Eighth, the content provider delivers the encrypted digital content to the user (step 24). The encrypted digital content may be delivered by downloading the encrypted digital content to the user's computer while the user is online at the content provider's web site, by attaching the digital content to an e-mail addressed to the user, or by shipping a disk containing the encrypted digital content to the user via a package courier. The user may pay for the digital

Additionally, page 9, lines 7-16 of the specification discloses:

within the vicinity of RDC. The RDC reads the user's PDK key and transmits data, along with the user's account number, acquired using conventional techniques, to the provider for verification. If more than one PDK key is read at RDC, either data from all PDK keys is transmitted to the provider or User Labels are displayed on a computer screen to enable the user to select the appropriate PDK key. The provider looks up the account record in its database using the transmitted account number and compares the transmitted PDK key data to information stored in the record. If a match is confirmed, the transaction/session is completed normally. If not confirmed, the transaction/session cannot be completed.

Among other portions of the specification, the above-identified section of the specification describes that the content provider transmits a first activation code received from the PDK to the key provider and that the key provider verifies if the first activation code is valid and informs the content provider. Based on the validation of the first activation code, the content provider marks a digital content requested by the PDK with a second activation code that is associated with the first activation code. Thus, amended claim 1 particularly points out and distinctly claims the subject matter regarded as the invention, so reconsideration and withdrawal of its rejection is respectfully requested.

As claims 3-5, 7 and 9-15 depend from claim 1, all arguments advanced above regarding independent claim 1 are also applicable to dependent claims 3-5, 7 and 9-15. Additionally, claim 3, 4, 7 and 13 are amended to convey a more clear scope according to the OA. Thus, reconsideration and withdrawal of the rejection of claims 3-5, 7 and 9-15 is respectfully requested.

Claim 8 is canceled, thereby obviating the basis for its rejection.

Response to Rejections Under 35 U.S.C. § 103

Claims 1, 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication No. 2002/0004783 to Paltenghe et al (herein, "Paltenghe") in view of US Patent Publication No. 2003/0195842 to Reece et al (herein, "Reece"). This rejection is overcome in view of the amended claims.

As amended, independent claim 1 recites in part:

> …a device coupled to the personal digital key via a wireless network, the device including a second wireless transceiver that receives a first activation code comprising a user label and an account number from the personal digital key and a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key provider, the device receiving digital content marked with an unlock code associated with the first activation code from a content provider responsive to the key provider authenticating the first activation code received from the personal digital key and the device receiving data from the key provider indicating whether the first activation code is authenticated.. (emphasis added)

The claimed invention recites a system comprising a tangible personal digital key and a device coupled to the personal digital key through a wireless network. The tangible

personal digital key includes a first wireless transceiver and the device includes a second wireless transceiver that receives a first activation code, including a user label and an account number, from the personal digital key. A reader/decoder circuit included in the device transmits the first activation code received from the personal digital key to a key provider and the device receives information from the provider authenticating the first activation code received from the personal digital key. Responsive to the key provider authenticating the first activation code, the device receives digital content marked with a unlock code associated with the first activation code from a content provider. Support for the amendments to claim 1 is found throughout the specification, for example at page 11, lines 7-22 and at page 9, lines 7-16.

Communication of a first activation code from the tangible personal key through the device to the key provider beneficially provides more flexible assignment, distribution and use of personal digital keys. Additionally, marking the requested digital content with an unlock code associated with the first activation code advantageously provides a second layer of security for the digital content.

The cited references fail to disclose at least the claimed elements of "the device receiving digital content marked with an unlock code associated with the first activation code from a content provider responsive to the key provider authenticating the first activation code received from the personal digital key," "a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key provider," and "the device receiving data from the key provider indicating whether the first activation code is authenticated."

Paltenghe fails to disclose "the device receiving digital content marked with an unlock code associated with the first activation code from a content provider responsive to the key provider authenticating the first activation code received from the personal digital key," as claimed. Rather, Paltenghe discloses a system used for information and financial banking including a virtual wallet including a local portion and a wallet server mirroring part of the content in the local portion of the virtual wallet. Paltenghe, Abstract, ¶ [0047]. Paltenghe sends a user's purchase request to a merchant using the local portion of the wallet and uses the wallet server to forward a payment request from the merchant back to the local portion of the wallet. Paltenghe merely discloses that the requests may be presented in the form of an invoice identifying purchase order information and accepted payment mechanisms. Paltenghe, ¶ [0071]. The purchase request and payment request disclosed by Paltenghe merely identify items for purchase and a payment mechanism, so there is no disclosure in Paltenghe of "the device receiving digital content marked with an unlock code associated with the first activation code from a content provider responsive to the key provider authenticating the first activation code received from the personal digital key."

Reece does not remedy the deficiency of Paltenghe. Rather, Reece discloses a system for using credit card processing infrastructure to make a value transaction over a network. Reece, Abstract. In Reece, a contact-less smart card is coupled to a PCB board using a radio frequency wireless link. Reece, ¶ [0082]. When a user seeks to make a purchase from an online merchant, a payment processing service provider receives a value from the smart card via the PCB board and communicates a limited use credit card number to the online merchant to affect the desired purchase. Reece, ¶ [0122]. Rather

than disclose "the device receiving digital content marked with an unlock code associated with the first activation code from a content provider responsive to the key provider authenticating the first activation code received from the personal digital key," as claimed, Reece discloses an online merchant receiving a credit card number used in a transaction and makes no disclosure of the online merchant, or of any device, "receiving digital content marked with an unlock code."

Additionally, Paltenghe fails to disclose "a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key provider," where the first activation code comprises "a user label and an account number from the personal digital key," as claimed. In addressing this element, the OA cites Figure 2, paragraphs [0017], [0019], [0045], [0046], [0052], [0054], [0058], [0073] and [0100] of Paltenghe. Figure 2 and its associated text of Paltenghe disclose:

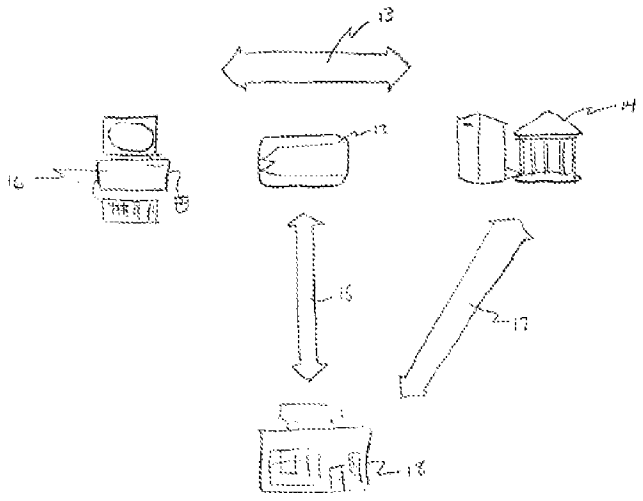

FIGURE 2

[0049] **FIG. 2** also provides a schematic depiction of a hybrid virtual wallet embodiment of the present invention and a method for using same. As shown in **FIG. 2**, a virtual wallet system may comprise a personal storage device **12**, an institutional server **14** and an interface device **16**. The personal storage device **12** and institutional server may each interact with the outside world, **18**.

[0052] The interface device need not include data but will generally include at least one of the following functions: user interface interacting; communicating; or public encryption. As will be understood from the foregoing discussion, where the personal storage device comprises a computer's hard disk and the interface device comprises the same computer, the interface device may include the data and functions of the personal storage device.

[0054] As shown in **FIG. 2** by the large arrow, personal storage device **12**, interface device **16** and institutional server **14** may communicate via secure interface interactions

13. In this regard, the interface device provides an interface between the personal storage device **12** and the institutional server **14**. Personal storage device **12** may communicate with outside world **18** for purpose of point of sale transactions **15**. These transactions include transactions involving the transfer of currency (e.g. a purchase) and also include transactions involving the transfer of personal information. The institutional server portion of the virtual wallet **14** may communicate with outside world **18** via intermediated internet transactions **17**. These transactions may be handled in a manner similar to current internet based transactions and involve both the transfer of financial information (financial banking) or personal information (information banking).

[0058] Protocols. Protocols include SET, Visa Cash, Mondex, OPS (see below). These will be definitions of how the wallet needs to interact with other systems and servers. Various system implementers will provide modules that implement these protocols.

Thus, Figure 2 of Paltenghe, and its associated text, discloses a virtual wallet system comprising a personal storage device communicating with an institutional server through an interface device. At most, the interface device disclosed by Paltenghe provides functions such as interaction with user interface, data communication and public encryption. While the claimed invention includes "a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key

provider," where the first activation code comprises "a user label and an account number from the personal digital key" Paltenghe merely discloses general communications between components of a virtual wallet and between other devices to identify items that are being purchased and describing payment for the items. Paltenghe, ¶ [0071].

Paragraphs [0017] and [0019] of Paltenghe disclose:

> [0017] Payment mechanisms stored in the virtual wallet may comprise bank account information, credit account information, electronic currency, electronic checks and debit cards, for example. Identity authentication mechanisms stored in the virtual wallet include personal identification information and authentication information. Personal identification information may comprise, for example, name, home address, work address, home phone, work phone, emergency contact information, and biometric information. Authentication information may comprise objects such as certificates, access keys and biometric information. Personal information and artifacts of the owner that are stored in the virtual wallet may comprise, for example, the personal identification information as stated above, other personal phone numbers and addresses, appointments and reminders, personal preferences and interests, loyalty credits, coupons, pictures, tokens and tickets. The above objects are just examples of some of the exhaustive capabilities of the virtual wallet. After reading this specification other examples will be obvious to those skilled in the art.
>
> [0019] Another advantage of a virtual wallet of the present invention is that the virtual wallet may advantageously be a trusted place to keep information and valuable financial items. Currently there are many founded and unfounded consumer fears regarding privacy and the safety of electronic transactions. If given a choice, it seems logical that consumers would rather store their sensitive information with someone that already has a reputation for trust and consumer advocacy than a suspicious third party. In a world where information is increasingly gathered on consumers in secret, marketed, and sold, an explicit policy of privacy protection and safety is a powerful inducement to hold a virtual wallet from a financial institution. Further, there is not only value in having consumer information, but value in moving it around as well. Also like money, information can be invested to provide—increasing returns. Information must also be protected, which give rise to the concepts of information vaults and safety deposit boxes. The central issue of privacy is turned into an opportunity, and is at the core of information banking.

Thus, paragraph [0017] of Paltenghe discloses payment mechanisms and identity authentication mechanisms stored in the virtual wallet. The disclosed payment

mechanisms include information, such as bank account information and credit account information. The disclosed identity authentication mechanisms include personal identification information and authentication information. Paragraph [0019] of Paltenghe merely discloses that the virtual wallet is a trusted place to keep information and financial items. Thus, like the remaining disclosure of Paltenghe, the cited paragraphs [0017] and [0019] also fail to disclose "a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key provider," where the first activation code comprises "a user label and an account number from the personal digital key," as claimed.

Paragraph [0045] and [0046] of Paltenghe disclose:

> [**0045**] **FIG. 1** depicts a possible embodiment of the present invention. Referring to **FIG. 1** according to the present invention a virtual wallet may comprise a hybrid between a wallet that resides locally with the owner, **2** and a wallet that resides remotely, such as with a server, **4**. A virtual wallet system further includes an interface, **6** between the local function, **2** and the server, **4**. The virtual wallet system may interact with the outside world, **8** through local wallet **2** and/or the server **4**. The hybrid virtual wallet combines the portability, owner control and minimized issuer resource aspects of a local wallet with the security and storage capability of a remote wallet. Thus, the hybrid virtual wallet advantageously optimizes the advantages of each type of residence. In the following discussion, the local residence or portion of the wallet may be referred to by these names or as a "client". The remote portion of the wallet may be referred to by this name or as a "server".

[0046] The local residence of the wallet may comprise, for example, the owner's personal computer, smart card, or other similar device that enables the wallet to be utilized off-line. Typically, the local aspect of the virtual wallet, the local contents, 3 comprises data and information determined by the wallet owner to be important, while the entire wallet is contained remotely. For example, the local aspect of the virtual wallet may comprise stored value purses, important personal and authentication information, and account information enabling the local aspect of the virtual wallet to emulate any of the functionality contained within the entire wallet. The owner advantageously is able to define and have access to the most important aspects of the wallet in a convenient package that can be remotely utilized. Preferably, the local aspect of the wallet is mirrored on the remote wallet or server, thus protecting the information in case the card has to be replaced. Additionally, the local aspect of the wallet comprises a certificate or other similar authentication instrument that allows the owner to remotely gain access to the entire virtual wallet on the server. Thus, the owner can still have access to all of the wallet functionality at sites where the local aspect of the wallet can be linked to the server.

While the claimed invention includes "a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key provider," where the first activation code "a user label and an account number from the personal digital key," paragraph [0045] of Paltenghe discloses a virtual wallet having a wallet residing locally with an owner, a server residing remotely and an interface between the local wallet and the server. While Paltenghe discloses that the local wallet and the server interact with outside world, there is no disclosure in Paltenghe of "a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key provider," where the first activation code comprises "a user label and an account number from the personal digital key," as claimed.

Paragraph [0046] of Paltenghe discloses information, such as personal and authentication information, value purses and account information, stored in the local wallet and partly mirrored on the remote server. However, the local wallet in Paltenghe merely includes a certificate allowing owner to access to the virtual wallet remotely.

Unlike the claimed activation code, the certificate disclosed by Paltenghe does not include "a user label and an account number." Accordingly, like the remaining disclosure of Paltenghe, the cited portions also fail to disclose "a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key provider," where the first activation code comprises "a user label and an account number from the personal digital key," as claimed.

Paragraph [0073] of Paltenghe discloses:

> [0073] FIG. 6 represents the feature where the wallet is opened for payment and a payment request is received by the wallet server. The payment request may be in any format, such as the SET initiation MIME, JCM (JAVA Commerce Message), and Open Trading Protocol (OTP) for example. When the wallet opens, the wallet owner or user must authenticate themself to the wallet so that the wallet knows the correct user is using the wallet interface. The user may authenticate themself utilizing biometric information, PIN and password, or other similar methods. Once the wallet authenticates the user, then the wallet and wallet server must mutually authenticate each other. When the various authentication's are complete, the invoice and payment mechanisms deriving from the payment request are presented to the wallet owner through the wallet server. The wallet owner views the information through the display of the wallet interface and sends the selected payment vehicle back through the wallet server.

Paragraph [0073] of Paltenghe discloses that the wallet opens and authenticates the user using biometric information, PIN and password or other similar methods, and that the wallet and the wallet server mutually authenticate each other. After completing authentication, the wallet server presents a user with a payment request to enable the user to relay a selected payment vehicle to the wallet server. Accordingly, Paltenghe fails to disclose an activation code comprising a user label and an account number or "a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key provider," as claimed.

Paragraph [0100] of Paltenghe discloses:

[0100] As depicted schematically in FIG. 11, the owner of virtual wallet 120 may utilize the smart card portion, 170 to complete electronic cash transactions 180, for example to pay a taxi fare 182. Smart card 170 may also be utilized in credit card transactions, 184 and 186. Smart card 170 is also a proxy 188 to the server 172 or network portion of the wallet through the internet, 190. A pass through interface allows the user to select an item (information or financial currency) from applications on the wallet server as if they were on the smart card. Since the applications and currency reside on the server, the number is not constrained by the size of the smart card's memory, and the card is easily replaced in the event of a mishap.

According to paragraph [0100] of Paltenghe, a smart card is used in electronic cash or credit card transactions as a proxy to the wallet server. Paragraph [0100] also discloses a pass-through interface used to select information or financial currency from applications on the wallet server. However, paragraph [0100] of Paltenghe merely discloses a technique for accessing data used by the wallet server and fails to disclose an activation code comprising a user label and an account number, much less "a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key provider," as claimed.

Reece does not remedy the deficiency of Paltenghe. Rather, Reece discloses a system for using credit card processing infrastructure to make a value transaction over a network. Reece, Abstract. In Reece, a contact-less smart card is coupled to a PCB board using a radio frequency wireless link. Reece, ¶ [0082]. When a user seeks to make a purchase from an online merchant, a payment processing service provider receives a value from the smart card via the PCB board and communicates a limited use credit card number to the online merchant to effect the desired purchase. Reece, ¶ [0122]. Rather than disclose "a reader/decoder circuit that transmits the first activation code received from the tangible personal digital key to a key provider," where the first activation code comprises "a user label and an account number from the personal digital key," as

claimed, Reece discloses a detector obtaining a predetermined value from a smart card and using the predetermined value to obtain a limited-used credit card for purchasing.

Furthermore, the cited references also fail to disclose or suggest "the device receiving data from the key provider indicating whether the first activation code is authenticated," as claimed.

Paltenghe does not disclose "the device receiving data from the key provider indicating whether the first activation code is authenticated," as claimed. While the OA cites Figure 2, paragraphs [0017], [0019], [0045], [0046], [0052], [0054], [0058], [0073] and [0100] of Paltenghe, which are reproduced above, neither these cited portions of Paltenghe nor the remaining disclosure of Paltenghe disclose "the device receiving information from the key provider authenticating the first activation code received from the personal digital key," as claimed.

Paragraph [0017] of Paltenghe discloses payment mechanisms and identity authentication mechanisms stored in the virtual wallet. The disclosed payment mechanisms include information, such as bank account information and credit account information. The disclosed identity authentication mechanisms include personal identification information and authentication information. Paragraph [0019] of Paltenghe merely discloses that the virtual wallet is a trusted place to keep information and financial items. Thus, like the remaining disclosure of Paltenghe, the cited paragraphs [0017] and [0019] also fail to disclose "the device receiving information from the key provider authenticating the first activation code received from the personal digital key," as claimed.

Paragraph [0045] of Paltenghe discloses a virtual wallet having a wallet residing locally with an owner, a server residing remotely and an interface between the local wallet and the server. While Paltenghe discloses that the local wallet and the server interact with outside world, there is no disclosure in Paltenghe of "the device receiving information from the key provider authenticating the first activation code received from the personal digital key," as claimed.

Paragraph [0046] of Paltenghe discloses information, such as personal and authentication information, value purses and account information, stored in the local wallet and partly mirrored on the remote server. However, the local wallet in Paltenghe merely includes a certificate allowing owner to access to the virtual wallet remotely. Accordingly, like the remaining disclosure of Paltenghe, the cited portions also fail to disclose "the device receiving information from the key provider authenticating the first activation code received from the personal digital key," as claimed.

Paragraph [0073] of Paltenghe discloses that the wallet opens and authenticates the user using biometric information, PIN and password or other similar methods, and that the wallet and the wallet server mutually authenticate each other. After completing authentication, the wallet server presents a user with a payment request to enable the user to relay a selected payment vehicle to the wallet server. Accordingly, Paltenghe fails to disclose "the device receiving information from the key provider authenticating the first activation code received from the personal digital key," as claimed.

Reece does not remedy the deficiency of Paltenghe. Rather, Reece discloses a system of using credit card processing infrastructure to make a value transaction over a network. Reece, Abstract. Rather, Reece discloses a system for using credit card

processing infrastructure to make a value transaction over a network. Reece, Abstract. In Reece, a contact-less smart card is coupled to a PCB board using a radio frequency wireless link. Reece, ¶ [0082]. When a user seeks to make a purchase from an online merchant, a payment processing service provider receives a value from the smart card via the PCB board and communicates a limited use credit card number to the online merchant to affect the desired purchase. Reece, ¶ [0122]. Thus, Reece does not disclose "the device receiving information from the key provider authenticating the first activation code received from the personal digital key," as claimed.

Accordingly, the cited references, whether taken alone or in combination, do not disclose or suggest every limitation of claim 1. Claim 1 is therefore patentable over the cited references. Hence, reconsideration and withdrawal of the rejection of claim 1 is respectfully requested.

As claim 5 depends from claim 1, dependent claim 5 is also patentably distinct from the cited references, whether taken alone or in combination, for at least the reasons presented above with respect to claim 1. Hence, reconsideration and withdrawal of its rejection is respectfully requested.

Claim 6 is canceled, thereby obviating the basis for its rejection.

Claims 3, 4 and 7-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Paltenghe and Reece as applied to claim 1 above, and further in view of US Patent Application No. 2001/0027439 ("Holtzman").

As claims 3, 4, 7 and 9-15 depend from claim 1, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claims 3, 4, 7 and 9-15.

Holtzman fails to remedy the deficient disclosure of Paltenghe and Reece. Rather, Holtzman discloses a computer-based system and method for completing a form requesting information about a user that is presented via a computer application program. Holtzman, Abstract. Holtzman at most obtains user information from an identifier included or generated by a token, such as a magnetic stripe card and a RFID tag. Holtzman matches the elements of user information with elements of requested information about the user in the form to complete the form. Holtzman, ¶ [0013]. Hence, Holtzman fails to disclose, or even suggest, at least the claimed elements of "responsive to the key provider authenticating the first activation code, the device receiving digital content from a content provider, the digital content marked with an unlock code associated with the first activation code," "a reader/decoder circuit that transmits the first activation code comprising a user label and an account number and the first activation code received from the tangible personal digital key to a key provider," and "the device receiving information from the key provider authenticating the first activation code received from the personal digital key."

Thus, claims 3, 4, and 7, 9-15 are patentably distinct from the cited references, both alone and in combination, and reconsideration and withdrawal of their rejection is respectfully requested.

Claim 8 is canceled, thereby obviating the basis for its rejection.

CONCLUSION

Allowance of all claims is requested. If the Examiner believes that direct contact will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,
JOHN J. GIOBBI

Dated: May 4, 2011 By: /Brian G. Brannon/

Brain G. Brannon Reg. No. 57,219
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9838
Fax: (801) 355-0160
Email: bbrannon@patentlawworks.net